Data Protection Information

Preface

We, Ehlers Moisch AI Data GbR, take the protection of your personal data seriously and would like to inform you here about data protection in our company.

As part of our data protection responsibility, additional obligations have been imposed on us by the entry into force of the EU General Data Protection Regulation (Regulation (EU) 2016/679; hereinafter: “GDPR”) to protect the personal data of the person affected by processing. (We will also address you as the affected person below as “customer”, “user”, “you”, “you” or “affected person”).

To the extent that we decide on the purposes and means of data processing either alone or jointly with others, this primarily includes the obligation to inform you transparently about the type, scope, purpose, duration and legal basis of the processing (see Articles 13 and 14 DS- GMOs). With this declaration (hereinafter: “Data Protection Notice”) we inform you about how your personal data is processed by us.

Our data protection information has a modular structure. They consist of a general part for all processing of personal data and processing situations that come into play every time a website is accessed (A. General) and a special part, the content of which only relates to the processing situation specified there with the name of the respective offer or product refers, to the visit to websites detailed here (e.g. visiting websites).

To be able to find the parts that are relevant to you, please note the following overview of the breakdown of the data protection information:

- Part A (General): Always relevant.
- Part B (Website and social media): Relevant if you use our website including our presence on social media.

A. General

(1) Definitions

Following the example of Art. 4 GDPR, this data protection notice is based on the following definitions:

- “Personal data” (Art. 4 No. 1 GDPR) is all information that relates to an identified or identifiable natural person (“data subject”). A person can be identified if they are directly or indirectly, by reference to an identifier such as a name, an identification number, an online identifier, location data or with the help of information about their physical, physiological, genetic, psychological, economic, cultural or social identity characteristics can be identified. Identification can also be achieved by linking such information or other additional knowledge. The origin, form or embodiment of the information is not important (photos, video or audio recordings can also contain personal data).
- “Processing” (Art. 4 No. 2 GDPR) is any process in which personal data is handled, whether with or without the help of automated (technology based) procedures. This includes the collection or procurement, recording, organization, ordering, storage, adaptation or modification, reading, querying, use, disclosure by transmission, distribution or other provision, comparison, the linking, restriction, deletion or destruction of personal data as well as the change of a goal or purpose on which data processing was originally based.

- “Controller” (Art. 4 No. 7 GDPR) is the natural or legal person, authority, institution or other body that alone or jointly with others decides on the purposes and means of processing personal data.
- “Third party” (Art. 4 No. 10 GDPR) is any natural or legal person, authority, institution or other body other than the data subject, the controller, the processor and the persons who are under the direct responsibility of the controller or processor are authorized to process the personal data; This also includes other legal entities belonging to the group.
- “Processor” (Art. 4 No. 8 GDPR) is a natural or legal person, authority, institution or other body that processes personal data on behalf of the person responsible, in particular in accordance with his instructions (e.g. IT service provider). In the sense of data protection law, a processor is not a third party.
- “Consent” (Art. 4 No. 11 GDPR) of the data subject means any voluntary, informed and unambiguous expression of will in the form of a statement or other clear confirmatory act for the specific case, with which the data subject consents understands that he or she agrees to the processing of personal data concerning him or her.

(2) Name and address of the person responsible for processing

We are the body responsible for processing your personal data within the meaning of Article 4 No. 7 GDPR:

Ehlers Moisch AI Data GbR

Bauerbergweg 14

22111 Hamburg

Contact: contact@pdfy.ai

For further information about our company, please see the legal notice on our website https://pdfy.ai/imprint.

(3) Legal basis for data processing

In principle, any processing of personal data is prohibited by law and is only permitted if the data processing falls under one of the following justifications:

- Art. 6 para . 1 sentence 1 lit. a GDPR ("consent"): If the data subject has voluntarily, informedly and unambiguously indicated by a statement or other clear confirmatory act that he or she consents to the processing of personal data concerning him or her for one or more specific purposes agrees;
- Art. 6 para . 1 sentence 1 lit. b GDPR : If the processing is necessary for the performance of a contract to which the data subject is a party or to carry out pre-contractual measures at the request of the data subject;
- Art. 6 para . 1 sentence 1 lit. c GDPR : If the processing is necessary to fulfill a legal obligation to which the controller is subject (e.g. B. a legal retention obligation);
- Art. 6 para . 1 sentence 1 lit. d GDPR : If processing is necessary to protect the vital interests of the data subject or another natural person;
- Art. 6 para . 1 sentence 1 lit. e GDPR : If the processing is necessary for the performance of a task that is in the public interest or in the exercise of official authority vested in the controller or
- Art. 6 para . 1 sentence 1 lit. f GDPR ("Legitimate interests"): If the processing is necessary to protect the legitimate (in particular legal or economic) interests of the controller or a third party, unless the conflicting interests or rights of the data subject outweigh them (in particular if this is the case). is a minor).

Storage of information in the end user's terminal equipment or access to information already stored in the end equipment is only permitted if covered by one of the following justifications:

- Section 25 Paragraph 1 TTDSG : If the end user has consented on the basis of clear and comprehensive information. The consent has according to Art. 6 Para. 1 Sentence 1 lit. a GDPR ;
- § 25 Para. 2 No. 1 TTDSG : If the sole purpose is to carry out the transmission of a message via a public telecommunications network or
- § 25 Para. 2 No. 2 TTDSG : If storage or access is absolutely necessary so that the provider of a telemedia service can provide a telemedia service expressly requested by the user.

Below we provide the applicable legal basis for the processing operations we carry out. Processing can also be based on several legal bases.

(4) Data deletion and storage period

For the processing operations we carry out, we indicate below how long the data will be stored by us and when it will be deleted or blocked. Unless an express storage period is stated below, your personal data will be deleted or blocked as soon as the purpose or legal basis for storage no longer applies. In principle, your data will only be stored on our servers in Germany, subject to any transfer in accordance with the regulations in A.(6) and A.(7).

However, storage may take place beyond the specified time in the event of an (imminent) legal dispute with you or other legal proceedings or if storage is required by legal regulations to which we as the controller are subject (e.g § 257 HGB , § 147 AO). If the storage period prescribed by statutory regulations expires, the personal data will be blocked or deleted, unless further storage by us is necessary and there is a legal basis for this.

(5) Data Security

We use appropriate technical and organizational security measures to protect your data against accidental or intentional manipulation, partial or complete loss, destruction or against unauthorized access by third parties (e.g. TSL encryption for our website), taking into account the state of the art and implementation costs and the nature, scope, context and purpose of the processing as well as the existing risks of a data breach (including their likelihood and impact) for the data subject. Our security measures are continuously improved in line with technological developments.

We will be happy to provide you with further information on this upon request.

(6) Collaboration with processors

As with every larger company, we also use external domestic and foreign service providers to handle our business transactions (e.g. for the areas of IT, logistics, telecommunications, sales and marketing). These only act according to our instructions and have been approved in accordance with Art. 28 GDPR compatible in addition obliged to comply with data protection regulations Regulations to comply .

(7) Requirements for the transfer of personal data to third countries

As part of our business relationships, your personal information may be shared or disclosed to third parties. These can also be located outside the European Economic Area (EEA), i.e. in third countries. Such processing takes place exclusively to fulfill contractual and business obligations and to maintain your business

relationship with us (legal basis is Art. 6 Para. 1 lit b or lit . f in conjunction with Article 44 ff. GDPR). We will inform you about the details of the transfer in the relevant places below.

The European Commission certifies that some third countries have data protection comparable to the EEA standard through so-called adequacy decisions (you can find a list of these countries and a copy of the adequacy decisions here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

However, in other third countries to which personal data may be transferred, there may not be a consistently high level of data protection due to a lack of legal regulations. If this is the case, we ensure that data protection is sufficiently guaranteed. This is possible via binding corporate regulations, standard contractual clauses of the European Commission for the protection of personal data in accordance with Article 46 Paragraph 1 and 2 lit. _ c GDPR (the 2021 Standard Contractual Clauses are available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0915&locale-en), certificates or recognized codes of conduct.

(8) No automated decision making (including profiling)

We do not intend to use personal data collected from you for any automated decision-making process (including profiling).

(9) No obligation to provide personal data

We do not make the conclusion of contracts with us dependent on you first providing us with personal data. In principle, you as a customer have no legal or contractual obligation to provide us with your personal data; However, it may be that we can only provide certain offers to a limited extent or not at all if you do not provide the necessary data. If this is exceptionally the case with the products we offer presented below, you will be informed of this separately.

(10) Legal obligation to transmit certain data

We may be subject to a special statutory or legal obligation to make lawfully processed personal data available to third parties, in particular public bodies (Art. 6 Para. 1 Sentence 1 Letter c GDPR).

(11) Your Rights

Assert your rights as a data subject regarding your processed personal data at any time using the contact details provided at the beginning under A. (2). As a data subject, you have the right:

- in accordance with Art. 15 GDPR, to request information about your data processed by us. In particular, you can obtain information about the purposes of processing, the category of data, the categories of recipients to whom your data has been or will be disclosed, the planned storage period, the existence of a right to correction, deletion, restriction of processing or objection, and the existence of a right to lodge a complaint , request the origin of your data, if it was not collected by us, as well as the existence of automated decision-making including profiling and, if necessary, meaningful information about its details;
- in accordance with Art. 16 GDPR, to immediately request the correction of incorrect data or the completion of your data stored by us;
- in accordance with Art. 17 GDPR , to request the deletion of your data stored by us, unless the processing is carried out to exercise the right to freedom of expression and information, to fulfill a

legal obligation, for reasons of public interest or to assert, exercise or defend is required by legal claims;

- in accordance with Art. 18 GDPR , to request the restriction of the processing of your data if you dispute the accuracy of the data or the processing is unlawful;
- in accordance with Art. 20 GDPR , to receive the data you have provided to us in a structured, common and machine-readable format or to request its transmission to another person responsible (“data portability”);
- to object to the processing in accordance with Art. 21 GDPR , provided that the processing is based on Art. 6 Para. 1 Sentence 1 lit. e or lit. f GDPR takes place. This is particularly the case if the processing is not necessary to fulfill a contract with you. Unless it is an objection to direct advertising, when exercising such an objection we ask you to explain the reasons why we should not process your data as we do. In the event of your justified objection, we will examine the situation and will either stop or adjust the data processing or show you our compelling legitimate reasons on the basis of which we continue the processing;
- in accordance with Art. 7 Para. 3 GDPR, your consent given once (also before the GDPR came into force, i.e. before May 25, 2018) - i.e. your voluntary, informed and unambiguous through a statement or other clear confirmatory This action makes it clear that you agree to the processing of the relevant personal data for one or more specific purposes - to revoke this to us at any time, if you have given such consent. This means that we are no longer allowed to continue the data processing that was based on this consent in the future
- in accordance with Art. 77 GDPR , to complain to a data protection supervisory authority about the processing of your personal data in our company, for example to the data protection supervisory authority responsible for us: Rodrigo Ehlers & Kevin Moisch, email : contact@pdfy.ai.

(12) Changes to the data protection information

As data protection law develops and technological or organizational changes occur, our data protection information is regularly checked for any need for adjustments or additions. You will be informed of any changes in particular on our German website at https://pdfy.ai. This data protection notice is valid as of November 2023.

B. Visiting our website and social media presence

(1) Explanation of the function

pdfy.ai offers a software solution as a service with which the user can interact via a user interface (chat) with the content of an input you have previously provided, such as a PDF document or text, using AI.

(2) Personal data processed

When you use the websites, we collect, store and process the following categories of personal data:

“Log data”: When you visit our websites, a so-called log data record (so-called server log files) is stored temporarily and anonymously on our web server. This consists of:

- the page from which the page was requested (so-called referrer URL)
- the name and URL of the requested page
- the date and time of the call
- the description of the type, language and version of the web browser used

- the IP address of the requesting computer, which is shortened so that a personal reference can no longer be established
- the amount of data transferred
- the operating system
- the message as to whether the call was successful (access status/Http status code)
- the GMT time zone difference

"Contact form data": When using contact forms, the data transmitted is processed (e.g. gender, last name and first name, address, company, email address and the time of transmission).

In addition to using our website, we offer subscription to our newsletter. If you register for our newsletter, the following “newsletter data” will be collected, stored and further processed by us:

- the page from which the page was requested (so-called referrer URL)
- the date and time of the call
- the description of the type of web browser used
- the IP address of the requesting computer, which is shortened so that a personal reference can no longer be established
- the E-Mail address
- the date and time of registration and confirmation

We would like to point out that we evaluate your user behavior when we send the newsletter. For this evaluation, the emails sent contain so-called web beacons or tracking pixels, which represent single-pixel image files that are stored on our website. For the evaluations, we link the above-mentioned data and the web beacons with your email address and an individual ID. Links contained in the newsletter also contain this ID. The data is only collected pseudonymously, ie . The IDs are therefore not linked to your other personal data, and direct personal reference is excluded.

If the user provides a document or makes an entry, the entire content, including any personal data contained therein, is recorded and stored on our servers (Supabase). These text parts are then transmitted to Microsoft Azure Open AI and put into a so-called embedding form. These embedding form text parts are in turn stored on our server.

(3) Purpose and legal basis of data processing

We process the personal data specified above in accordance with the provisions of the GDPR and other relevant data protection regulations and only to the extent necessary. Insofar as the processing of personal data is based on Art. 6 Para . 1 Sentence 1 lit. f GDPR , the purposes mentioned also represent our legitimate interests.

The processing of the log data serves statistical purposes and to improve the quality of our website, in particular the stability and security of the connection (legal basis is Art. 6 Para. 1 S. 1 lit. a or lit. f GDPR).

Contact form data is processed to process customer inquiries (legal basis is Art. 6 Para. 1 S. 1 lit. b or lit. f GDPR).

The newsletter data is processed for the purpose of sending the newsletter. When you register for our newsletter, you consent to the processing of your personal data (legal basis is Art. 6 Para. 1 lit. _ a GDPR). To register for our newsletter we use the so-called double opt-in procedure . This means that after you register, we will send you an email to the email address you provided, in which we will ask you to confirm that you would like to receive the newsletter. The purpose of this procedure is to be able to prove your registration and, if necessary, to clarify any possible misuse of your personal data. You can revoke your consent to receive the newsletter at any time and unsubscribe from the newsletter. You can declare your revocation by clicking on the link provided in every newsletter email, by email to contact@pdfy.ai or by sending a message to the contact details provided in the legal notice.

If the storage of information in your end device or access to information that is already stored in the end device is necessary for the processing of the data, Section 25 Paragraphs 1 and 2 TTDSG is the legal basis for this.

The processing of personal data containing the documents and inputs provided by users is carried out for the purpose of fulfilling the contract (Art. 6 I lit. a. GDPR) and only takes place with express consent (Art. 6 I lit. b . GDPR).

(4) Duration of data processing

Your data will only be processed for as long as necessary to achieve the processing purposes mentioned above; The legal bases specified in the context of the processing purposes apply accordingly. Regarding the use and storage period of cookies, please note point A. (5) and the cookie policy https://pdfy.ai/legal/cookies.pdf.

Third parties used by us will store your data on their system for as long as is necessary in connection with the provision of services for us in accordance with the respective order.

You can find more information about the storage period under A. (5) and the cookie policy https://pdfy.ai/legal/cookies.pdf.

(5) transfer of personal data to third parties; Basis of justification

The following categories of recipients, who are usually processors (see A. (6)), may have access to your personal data:

- Service providers for the operation of our website and the processing of the data stored or transmitted by the systems (e.g. for data center services, payment processing, IT security). The legal basis for the transfer is then Art. 6 Para . 1 Sentence 1 lit. b or lit. f DS-GVO , as long as it does not involve contract processors;
- State bodies/authorities, insofar as this is necessary to fulfill a legal obligation. The legal basis for the transfer is then Art. 6 Para . 1 Sentence 1 lit. c GDPR ;
- Persons employed to carry out our business operations (e.g. auditors, banks, insurance companies, legal advisors, supervisory authorities, those involved in company acquisitions or the establishment of joint ventures). The legal basis for the transfer is then Art. 6 Para . 1 Sentence 1 lit. b or lit. f GDPR .

For the guarantees of an appropriate level of data protection when data is transferred to third countries, see A. (7).

We only pass on your personal data to third parties if you do so in accordance with Art. 6 Para. 1 Sentence 1 lit. a GDPR you have given your express consent to this.

(6) Use of cookies, plugins and other services on our website:

a) Cookies

We use cookies on our websites. Cookies are small text files that are assigned and stored on your hard drive by the browser you are using using a characteristic string and through which certain information flows to the place that sets the cookie. Cookies cannot run programs or transmit viruses to your computer and therefore cannot cause any harm. They serve to make the Internet offering more user-friendly and effective overall, i.e. more pleasant for you.

Cookies can contain data that makes it possible to recognize the device used. In some cases, cookies only contain information about certain settings that are not personally identifiable. However, cookies cannot directly identify a user.

A distinction is made between session cookies, which are deleted as soon as you close your browser, and permanent cookies, which are stored beyond the individual session. In terms of their function, cookies are differentiated between:

- Technical cookies: These are absolutely necessary to move around the website, use basic functions and ensure the security of the website; they do not collect information about you for marketing purposes or remember which websites you have visited;
- Performance cookies: These collect information about how you use our website, which pages you visit and, for example , whether errors occur when using the website; they do not collect any information that could identify you - all information collected is anonymous and is only used to improve our website and find out what interests our users;
- Advertising cookies, targeting cookies: These are used to offer the website user tailored advertising on the website or offers from third parties and to measure the effectiveness of these offers; Advertising and targeting cookies are stored for a maximum of 13 months;
- Sharing cookies: These serve to improve the interactivity of our website with other services (e.g. social networks); Sharing cookies are stored for a maximum of 13 months.

The legal basis for cookies, which are absolutely necessary to provide you with the expressly requested service, is Section 25 Paragraph 2 No. 2 TTDSG . Any use of cookies that is not absolutely technically necessary represents data processing that can only be carried out with your express and active consent in accordance with Section 25 Paragraph 1 TTDSG iVm Art. 6 para . 1 sentence 1 lit. a GDPR is permitted. This applies in particular to the use of performance, advertising, targeting or sharing cookies. In addition, we only pass on your personal data processed through cookies to third parties if you do so in accordance with Art. 6 Para. 1 Sentence 1 lit. a GDPR you have given your express consent to this.

b) Cookie Policy

For more information about which cookies we use and how you can manage your cookie settings and opt out of certain types of tracking, please see our Cookie Policy https://pdfy.ai/legal/cookies.pdf

c) Microsoft Azure Open AI

Azure Open AI processes the documents provided by the user as well as the queries entered for them. We transfer personal data to Microsoft Azure Open AI. The data will be stored within the framework of the legal

requirements of the GDPR and deleted in compliance with the provisions of Art. 17 GDPR. The data is processed in the European Union. We have concluded a contract with Microsoft Azure for order processing in accordance with Art. 28 GDPR. Microsoft will therefore only use all information for a strictly intended purpose in order to evaluate the use of our websites for us and to compile reports on website activity.

The data processing conditions (Data Processing Addendum), which correspond to the standard contractual clauses, can be found at: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA. For more information, see: https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy?context=%2Fazure%2Fcognitive-services%2Fopenai%2Fcontext%2Fcontext

d) Supabase

Supabase is a hosting provider that includes our database, users' original files (PDFs) and authentication.

For authentication, Supabase stores the email used and a unidirectional (hashed) encrypted form of the password set. Supabase also handles email traffic for emails that are relevant to authentication.

We store the following data in our database:

- User's email
- The display name
- The text content of the uploaded files
- Chat messages exchanged with the AI in the UI, as well as the reply messages from ChatGPT (OpenAI)

Website: https://supabase.com/
Data Privacy: https://supabase.com/privacy

The data processing conditions (Data Processing Addendum), which correspond to the standard contractual clauses, can be found at: https://supabase.com/legal/dpa

e) Sentry

Sentry is a tool that allows developers to monitor and fix crashes in programming code in real time. The tool also offers in-depth context for all detected errors and thus a high level of error transparency. This allows companies to efficiently resolve serious code inconsistencies

We use Sentry, an error management tool, for our services. The service provider is the American company Sentry Inc., San Francisco, 132 Hawthorne St. San Francisco, USA

In order to ensure the technical stability of a website, we collect user data such as:

- IP address,
- information about the device,
- Information about the browser used and
- Any steps that led to a technical error in the code (including stack trace).

Sentry also processes your data in the USA, among other places. We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. This can pose various risks to the lawfulness and security of data processing.

Sentry uses so-called standard contractual clauses (Article 46, Paragraphs 2 and 3 of the GDPR) as the basis for data processing for recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or for data transfer there. Standard Contractual Clauses (Standard Contractual Clauses SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through this clause, Sentry undertakes to comply with European data protection standards when processing its relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here, among others: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0915&locale-en

The Data Processing Addendum, which corresponds to the standard contractual clauses, can be found at: https://sentry.io/legal/d p a/

You can find out more about the data processed through the use of Sentry in the data protection declaration at: https://sentry.io/privacy/

f) Vercel

We use Vercel , a cloud deployment platform, for our services. The service provider is the American company Vercel Inc., 340 S Lemon Ave, 4133 , Walnut , CA 91789, USA

The following data is transferred to Vercel :

- Date and time of access
- IP address of the requesting computer
- Name and URL of the retrieved file
- Amount of data transferred
- Message as to whether the retrieval was successful
- Recognition data of the browser and operating system used
- Website from which access is made
- Name of the Internet access provider

Vercel also processes your data in the USA, among other places. We would like to point out that, according to the European Court of Justice, there is currently no adequate level of protection for data transfer to the USA. This can pose various risks to the lawfulness and security of data processing.

Vercel uses so-called standard contractual clauses (Article 46, Paragraphs 2 and 3 of the GDPR) as the basis for data processing for recipients based in third countries (outside the European Union, Iceland, Liechtenstein, Norway, i.e. in particular in the USA) or for data transfer there. Standard Contractual Clauses (Standard Contractual Clauses SCC) are templates provided by the EU Commission and are intended to ensure that your data complies with European data protection standards even if it is transferred to third countries (such as the USA) and stored there. Through this clause, Vercel undertakes to comply with the European level of data

protection when processing its relevant data, even if the data is stored, processed and managed in the USA. These clauses are based on an implementing decision of the EU Commission. You can find the resolution and the corresponding standard contractual clauses here, among others: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0915&lo c ale-en

The data processing conditions (Data Processing Addendum), which correspond to the standard contractual clauses, can be found at: https://vercel.com/legal/Vercel_Inc_-_Data_Processing_Addendum.pdf

You can find out more about the data processed through the use of Vercel in the data protection declaration at: https://vercel.com/legal/privacy-policy.

g) Digital Ocean

Digital Ocean is a cloud service and is our hosting provider for our API. The service provider is the American company DigitalOcean LLC, New York, NY, 101 6thAve, USA

The following data is transmitted:

- Date and time of access
- IP address of the requesting computer
- Name and URL of the retrieved file
- Amount of data transferred
- Message as to whether the retrieval was successful
- Recognition data of the browser and operating system used
- Website from which access is made
- Name of the Internet access provider

The data processing conditions (Data Processing Addendum), which correspond to the standard contractual clauses, can be found at: https://www.digitalocean.com/legal/data-processing-agreement.

You can find out more about the data processed using Digital Ocean in the data protection declaration at: https://www.digitalocean.com/legal/privacy-policy.

h) Stripe

The company Stripe offers payment solutions for online payments. For users within the EU, Stripe Payments Europe Ltd. 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland.

The personal data collected are:

- Tracker,
- usage data,
- First name,
- Last name,
- E-mail address,
- different types of data as specified in the privacy policy of the service,
- Billing address,
- payment information,

- Purchase history.

We have concluded a contract with Stripe for order processing in accordance with Art. 28 GDPR. Stripe will therefore only use all information for a strictly intended purpose to evaluate the use of our websites for us and to compile reports on website activity.

The data processing conditions (Data Processing Addendum), which correspond to the standard contractual clauses, can be found at: https://stripe.com/at/legal/dpa.

You can find out more about the data processed using Digital Ocean in the data protection declaration at: https://stripe.com/at/privacy.

i) Hotjar

The company Hotjar Ltd. offers services to measure our app performance and user behaviour analytics. The service provider is Hotjar Ltd., Dragonara Business center 5. floor, Dragonara Road, Paceville St. Julian's STJ 3141 Malta

The personal data collected are:

- Device's IP address (captured and stored only in anonymized form)
- Device screen size Device type (unique device identifiers)
- Browser information
- Geographic location (country only)
- Preferred language used to display the website.

The data processing conditions (Data Processing Addendum), which correspond to the standard contractual clauses, can be found at: https://www.hotjar.com/de/legal/support/dpa/.

You can find more about how the data is processed at https://www.hotjar.com/legal/policies/privacy/.

j) Postmark (ActiveCampaign LLC)

In utilizing Postmark for our email communication services, we are committed to upholding the high standards of data protection mandated by the EU's General Data Protection Regulation (GDPR). We confirm Postmark's compliance with GDPR, which guarantees the safety and privacy of personal data.

Data Processing and Enhanced Security

Processed Data

Personal data that is shared with Postmark:

- Email of the user.
- Chosen display name (not necessarily real name) of the user.
    - The display name can be updated in the application settings.

Data Centers:

- Our emails are managed through Postmark's infrastructure, hosted at Deft's data center in the U.S. and Amazon Web Services (AWS). These centers are fortified with top-tier security features including SOC 2 Type 2 certification, biometric scanning, and 24/7 monitoring.
- Robust Security Measures:
    - Data Encryption: We encrypt all data sent to Postmark using SSL. Additionally, we secure stored data with 2048-bit RSA encryption.
    - Access Control: Access to personal data is strictly regulated, available only to authorized staff under strict confidentiality commitments.
    - Application Security: The Postmark platform, including its API and SMTP services, employs SSL/TLS encryption. We ensure that passwords are securely hashed, and are inaccessible even to Postmark's team.

Data Retention Policy

Postmark stores email content and related metadata for 45 days, facilitating customer access to message history. Post this duration, the data is purged. Nevertheless, data regarding email bounces, spam complaints, and unsubscribes is kept indefinitely for analytical purposes.

Handling Data Subject Requests

In line with GDPR, Postmark offers efficient tools for responding to data subject requests. This encompasses automated tools for data deletion via their Data Removal API, and options to modify data retention through the Retention Add-On.

Data Processing Addendum (DPA)

We adhere to Postmark’s DPA, which incorporates the latest Standard Contractual Clauses for international data transfers in compliance with GDPR.

Sub-processors Management

Postmark engages sub-processors like AWS and Deft for hosting services. We are promptly informed of any sub-processor changes, preserving our right to object to new sub-processors.

Contact for Data Privacy Inquiries

For queries or concerns about our data privacy and security measures with Postmark, please reach out to us at contact@pdfy.ai.

k) Deepgram

Deepgram specializes in Automatic Speech Recognition (ASR) services, primarily for transcribing audio files using advanced deep learning models. This section of the privacy policy addresses the handling of information related to the audio files of users processed by Deepgram.

Collection and Use of User Audio Files

- User Content: Deepgram collects and stores personal information contained within the audio files uploaded or transmitted by users as part of the Service. This includes any data within the audio files that may qualify as personal information.

- Purpose of Collection: The primary use of this data is to provide ASR services, including transcription and analysis of audio content.

Data Processing and Storage

- Deepgram acts as a data processor for the audio files provided by users. The processing of this data is carried out solely for the purpose of delivering ASR services.
- Customer Data: Deepgram processes audio files as per the instructions of its customers, who are the data controllers. Deepgram's role does not extend beyond this scope in relation to the personal information contained in the audio files.

Data Retention

The retention and deletion of data contained within audio files are governed by the agreement between Deepgram and its business customers, in alignment with legal and contractual requirements.

Third-Party Involvement

There may be instances where third-party service providers are used to facilitate the processing of audio files. In such cases, these providers are bound by confidentiality agreements and data processing terms that align with Deepgram's privacy commitments.

Compliance and Legal Obligations

As a data processor, Deepgram ensures compliance with relevant data protection regulations, including GDPR, in the context of processing user audio files.

Contact Information

For specific inquiries related to the processing of audio files contact us at contact@pdfy.ai.